DETAILED ACTION

Allowable Subject Matter

1. **Claims 1, 2, 7, 53, 60, 61, and 63-70** are allowed.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Authorization for this examiner's amendment was given in a telephone interview with Leonard Searcy II on 2/17/10.The application has been amended as follows:

The claims have been amended as follows:

In claims 56-60:

Claims 56-60 have been cancelled.

In claim Claim 60 :

Claim 60 has been amended as follows:

60. (Currently Amended) The method [network] of claim [59] 7, further comprising the one or more cryptographic methods implemented in a secure relationship maintained by a MAC Security Key Agreement.

Please change Claim 66 to read:

66. (Previously Presented) An access point for segregating traffic among a plurality of end stations, comprising:

one or more storage units configurable to store:

a frame having a cryptographic authentication code; the frame having a source media access control (MAC) address to determine a preliminary VLAN classification when the frame carries a null virtual LAN ID;

the frame having a virtual LAN ID (VID) as the preliminary VLAN classification when the frame carries the VID;

a table of security associations providing a cryptographic authentication code key based on the preliminary VLAN classification wherein the cryptographic authentication code key is used to recompute a new cryptographic authentication code over a payload of the frame;

a processor configured to compare the new cryptographic authentication code ~~[compared]~~ with the cryptographic authentication code;

implement the preliminary VLAN classification ~~[implemented]~~ as a final VLAN classification when the new cryptographic authentication code and the cryptographic authentication code match, wherein the frame is decrypted; and

not implement the preliminary VLAN classification ~~[not implemented]~~ as the final VLAN classification when the new cryptographic authentication code and the cryptographic authentication code do not match, wherein the frame is discarded; and discard the frame when said VLAN classification is not implemented.

Claims Appendix

In accordance with prosecution history, claims 51 and 52 were added in amendments filed 10/2/2007, but these claims were inadvertently omitted in the following amendments. As per a telephone interview with applicant's representative, the listing of the claims are shown in following:

1. (Previously Presented) An access point device for a wireless LAN for isolating an end station from a plurality of end stations to support segregation of network traffic between the end station and the plurality of end stations, the access point device serving as a common access point for communication in the wireless LAN, the access point device configured to:

receive a request from said end station that is an association request or a probe request; and

process said request by:

determining for said request a basic service set (BSS) that is unknown to said access point device at the time of receipt of said request by said access point device;

receiving at least one parameter defining said BSS;

establishing said BSS based at least on said at least one parameter;

establishing a security association with said end station within said BSS wherein the security association includes at least two keys, one key for encryption and another key for computing an authentication code; and

sending a response to said end station that includes a BSSID of said established BSS.

2. (Previously presented) The access point device of Claim 1, further configured to provision a plurality of separate LAN segments while providing separate link privacy and integrity for each of said LAN segments.

3-6. (Canceled)

7. (Previously Presented) A method in an access point device for a secure wireless network to support segregation of network traffic among a plurality of stations, each of said stations having a hardware (MAC) address, comprising:

receiving an association request or a probe request from a first station;

determining for said request a basic service set (BSS) that is unknown to said access point device at the time said request was received by said access point device;

receiving at least one parameter which defines said BSS;

establishing said BSS based at least on said at least one parameter, thereby creating the Basic Service Set (BSS) for a subset of said stations;

establishing a security association with each of said end stations within said BSS wherein the security association includes at least two keys, one key for encryption and another key for computing an authentication code; and

sending a response to said end station that includes a BSSID of said established BSS,

wherein stations in said subset belong to said established BSS and share a group security association.

8-50. (Canceled)

51. (Previously presented) The access point device of Claim 1 wherein said at least one parameter is provided by said end station.

52. (Previously presented) The access point device of Claim 1 wherein said at least one parameter is provided by a source other than said end station.

53. (Previously presented) The access point device of Claim 1 wherein said request includes an SSID (service set identifier), wherein said at least one parameter is based on said SSID.

54-55. (Canceled)

56. (Previously presented) A secure wireless network, comprising:

a virtual 802.11 Basic Service Set (BSS);

a plurality of stations in the virtual BSS, each of said stations having a hardware media access control (MAC) address;

all said stations in said virtual BSS sharing a group security association wherein said group security association is an implementation of a MAC security; and

one of said stations in said virtual BSS comprising a public access point which is a physical access point.

57. (Previously Presented) The network of claim 56, wherein said implementation of said MAC security comprises said implementation of a secure MAC service.

58. (Previously Presented) The network of claim 57, wherein said implementation of said secure MAC service comprises a MAC Security Key Agreement and a MAC Security Entity.

59. (Previously Presented) The network of claim 57, wherein said group security association comprises using one or more cryptographic methods.

60. (Previously Presented) The network of claim 59, further comprising the one or more cryptographic methods implemented in a security relationship maintained by a MAC Security Key Agreement.

61. (Previously Presented) A method in an access point device for a secure wireless network to support segregation of network traffic among a plurality of stations, each of said stations having a hardware media access control (MAC) address, comprising:

receiving an association request or a probe request from a first station;

determining for said request a basic service set (BSS) that is unknown to said access point device at a time said request was received by said access point device;

receiving at least one parameter which defines said BSS;

establishing said BSS based at least on said at least one parameter, thereby creating said BSS for a subset of said stations; and

sending a response to said end station that includes a BSSID of said established BSS;

wherein stations in said subset belong to said established BSS and share a group security association wherein said group security association is an implementation of a MAC security wherein said implementation of said MAC security comprises said implementation of a secure MAC service.

62. (Canceled)

63. (Previously Presented) The method of claim 61, wherein said implementation of said secure MAC service comprises a MAC Security Key Agreement and a MAC Security Entity.

64. (Previously Presented) The method of claim 61, wherein said group security association comprises using one or more cryptographic methods.

65. (Previously Presented) The method of claim 64, further comprising the one or more cryptographic methods implemented in a security relationship maintained by a MAC Security Key Agreement.

66. (Previously Presented) An access point for segregating traffic among a plurality of end stations, comprising:

one or more storage units configurable to store:

a frame having a cryptographic authentication code;

the frame having a source media access control (MAC) address to determine a preliminary VLAN classification when the frame carries a null virtual LAN ID;

the frame having a virtual LAN ID (VID) as the preliminary VLAN classification when the frame carries the VID;

a table of security associations providing a cryptographic authentication code key based on the preliminary VLAN classification wherein the cryptographic authentication code key is used to recompute a new cryptographic authentication code over a payload of the frame;

the new cryptographic authentication code compared with the cryptographic authentication code;

the preliminary VLAN classification implemented as a final VLAN classification when the new cryptographic authentication code and the cryptographic authentication code match, wherein the frame is decrypted; and

the preliminary VLAN classification not implemented as the final VLAN classification when the new cryptographic authentication code and the cryptographic authentication code do not match, wherein the frame is discarded.

67. (Previously Presented) The access point of claim 66, wherein the access point is configurable to perform an authentication operation that generates the authentication code key.

68. (Previously Presented) The access point of claim 66, wherein the new cryptographic authentication code is recomputed over the payload using a cryptographic message digest algorithm determined during an initial authentication operation.

69. (Previously Presented) The access point of claim 66, wherein the final VLAN classification is used as a value of a VLAN classification parameter of any corresponding data request primitives.

70. (Previously Presented) The access point of claim 66, wherein the cryptographic authentication code or the new cryptographic authentication code uniquely identifies the VLAN.

Allowable Subject Matter

3. The following is an examiner's statement of reasons for allowance:
Concerning claims 1, 2, 7, 53, 60, 61, and 63-70, prior art fails to teach a method in an access point device for a secure wireless network to support segregation of network traffic among a plurality of stations, each of said stations having a hardware (MAC) address, comprising: receiving an association request or a probe request from a first station; determining for said request a basic service set (BSS) that is unknown to said access point device at the time said request was received by said access point device; receiving at least one parameter which defines said BSS; establishing said BSS based at least on said at least one parameter, thereby creating the

Basic Service Set (BSS) for a subset of said stations; establishing a security association with each of said end stations within said BSS wherein the security association includes at least two keys, one key for encryption and another key for computing an authentication code; and sending a response to said end station that includes a BSSID of said established BSS, wherein stations in said subset belong to said established BSS and share a group security association.

Kitchin is an exemplary reference from a relevant subclass. Kitchin is discussing a system and method for permitting communication between subscribers in a wireless network and devices coupled to one or more wired communication networks. A transceiver circuit transmits data to or receives data from one or more subscribers through a wireless transmission medium. A first data link control (DLC) circuit is adapted to transmit data between the transceiver circuit and one or more devices coupled to a first wired communication network. A second DLC circuit is adapted to transmit data between the transceiver circuit and one or more devices coupled to a second wired communication network.

Halasz is also an exemplary reference from a relevant subclass. Halasz is discussing a system for providing a Virtual Local Area Network (VLAN) by use of an encryption states or encryption keys for identifying a VLAN. A table of data including a VLAN and an associated encryption state or key is provided for assignment of encryption states or keys, for devices in a wireless local area network.

Further, Meier is an exemplary reference from a relevant subclass. Meier is discussing a communication system in which multiple protocols and proxy services are executed by an access point. In one embodiment, GVRP and GMRP registrations are combined in a single packet when

a wireless device roams to a different VLAN. In addition, outbound GVRP and GMRP multicast messages are handled by an access point such that the wireless device is not burdened with the associated computational overhead. In a further embodiment, a wireless device may dynamically switch between a VLAN-aware state and a VLAN-unaware state depending on the nature of a detected access point. For example, if a relevant access point supports GVRP, the wireless device may operate as a VLAN terminal. If a wireless device is not attached to an access point with a matching VLAN ID, the wireless device sends and receives VLAN tagged frames. If a wireless device configured with a VLAN ID is attached to an access point with a matching VLAN ID, or if the wireless device is attached to a non-VLAN access point, then the wireless device may send and receive raw/untagged frames. In another embodiment, a special ID that is different than the native VLAN ID for a switch port is used for VLAN-unaware devices. This allows such devices that do not issue tagged frames to belong to a single VLAN ID.

Therefore, regarding claims 1, 2, 7, 53, 60, 61, and 63-70, prior art fails to teach a method in an access point device for a secure wireless network to support segregation of network traffic among a plurality of stations, each of said stations having a hardware (MAC) address, comprising:

receiving an association request or a probe request from a first station; determining for said request a basic service set (BSS) that is unknown to said access point device at the time said request was received by said access point device; receiving at least one parameter which defines said BSS; establishing said BSS based at least on said at least one parameter, thereby creating the Basic Service Set (BSS) for a subset of said stations; establishing a security association with each of said end stations within said BSS wherein the security association includes at least two

keys, one key for encryption and another key for computing an authentication code; and sending a response to said end station that includes a BSSID of said established BSS, wherein stations in said subset belong to said established BSS and share a group security association.

Conclusion

4. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to:**

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window

Randolph Building

401 Dulany Street

Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shannon Brooks whose telephone number is (571) 270-1115. The examiner can normally be reached on 7:30a.m. to 5p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nick Corsaro can be reached on (571) 272-7876. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

/Shannon R. Brooks/

Examiner, Art Unit 2617

Shannon Brooks

February 17, 2010

/NICK CORSARO/

Supervisory Patent Examiner, Art Unit 2617